REMARKS

Reconsideration of the above-identified application, as amended, is respectfully requested.

In the Official Action dated April 2, 2004, the Examiner first indicated that drawing Figure 1 should be labeled as "Prior Art". Applicants hereby submit a proposed amendment to drawing Figure 1 in compliance.

Further in the Office Action, the Examiner rejected Claims 1-21 under 35 U.S.C. 102(e) as being allegedly anticipated by Hurtado et al. (US 6,611,812).

Applicants respectfully disagree, primarily for the reason that Hurtado requires distribution of a new player application for each end-user. This is in accordance with prior art techniques, for example, where a new version of a user application (e.g., iTunes) is required to be provided to an end-user, that is enabled to handle secure containers (e.g., encrypted music) that requires a user to buy keys, for example to unlock the containers.

In the present invention, there is provided a technique that enables use of an existing, off-the-shelf player application (e.g., iTunes), and providing a trusted content handler (TCH) element that sits between the disc (having music content, for example) and the current, unmodified version of the player application (e.g., iTunes) that decrypts the content. As part of this system of the invention, there is provided a verification mechanism that enables the TCH to trust the iTunes player application, and verify that it is not a "rogue" player application that will illegally save and/or distribute the content to the Internet, for example, and, that will prevent the user to access or save the protected content when not granted such user rights. Thus, the player application will identify a piece of music or file, and the TCH, local to the end-user device, will decide whether to provide the player application with that file.

In contrast, according to the prior art technique as embodied and taught in Hurtado, a trusted player is provided, e.g., a iTunes player application, that has been modified to read content, and then an Internet distribution site will send secure containers down to the player.

Respectfully, Claims 1, 6 and 10 of the present invention clearly sets forth this distinction and further distinguishes over Hurtado in the following respects: First, the claimed verification system element to validate the integrity of the player applications is neither taught nor suggested in Hurtado. In the iTunes player application example described herein, this verification system element would function to verify that the TCH is talking to the off-the-shelf iTunes player application (or any other player app. such as a web-browser) and not one that has been modified to cipher off content illegally. This is clearly described in the specification at page 9, lines 32-page 16, line 17 in which an off-line process is used to generate a digital trust certificate that attests to a property of the off-the-shelf player application (set forth in Claim 2), and the verification system that verifies that a particular player application is certified as a trusted app. before digital content is distributed to it (set forth in Claims 3 and 4). As described at page 11, lines 20-27, the off-line verification process essentially scans the player applications code modules to result in the generation of a trust certificate that includes the signed digest(s) of the application code modules. The verification system then verifies that the player application on the end-user client is certified as a trusted application to handle protected content entrusted to it. Thus, in one embodiment of the invention, as described in the specification at page 11, lines 12-18, before launching the player application, the verification system at that time verifies the integrity of the code by applying a message digest algorithm to the code module in question and comparing the result to the pre-signed digest. An exact match means that the code installed on the client is identical to the one certified (Trust Certificate), and hence is safe to handle the

content entrusted to it. Thus, the integrity of the application is verified in the present invention which is neither taught nor suggested in Hurtado.

Respectfully, the Examiner's reliance on Hurtado citing Figure 1c) and at Col. 13, lines 44-54, is misplaced. This passage cited in Hurtado actually does not teach validation of integrity of a player application, but rather deals with some (commerce) transaction integrity (e.g., sale or distribution of music to end-user), but not the integrity of the player application itself. Hurtado actually teaches use of an end-user client device that is part of the Digital Rights Management (DRM) system itself, by its holding of a key (that would be different for every end-user player application according to Hurtado's teachings), for example, and that is not related to the integrity of the player application, but only indicates to the system that the end-user client is to be trusted by its knowledge of a "secret", e.g., a key.

To visualize this difference, Hurtado teaches a player application and DRM part including content encryption/decryption function that would be in one secure "box". The present invention essentially has broken the box into two parts: a player part comprising an off-the-shelf player application outside the DRM system, and the DRM part (verification system authenticator, Trusted Content Handler (TCH)). Only the trusted content handler interfaces with the Clearinghouse and holds a secret "key" for example.

Second, with respect to the claimed Trusted Content Handler element of present Claim 1 of the invention, Hurtado further does not teach this element. The Examiner alleges Hurtado's notion of a "secure container" and its use of keys for decrypting encrypted content teaches the trusted content handler element of the invention. However, respectfully, Hurtado's secure container it is actually an encrypted file, and is not active or embedded with intelligence for making decisions. Thus, in Hurtado, the secure end-user player application will know how to

open the secure container because of its possession of a key (different for each end-user device). The TCH of the present Claim 1, will have a mechanism that possesses a key, however, the distinction is that the trusted player is separate and distinct from the content handler, wherein Hurtado these are part of the same system. Moreover, in the present invention as claimed, the content decrypted by the TCH is transmitted to the player applications via the player application's defined extension mechanism and this provides transparency to the player application. This extension mechanism is akin to the protocol handler provided in a web-browser (e.g., Internet Explorer application) that are different for handling FTP, or HTTP protocols, for example. This notion of transparency using extension mechanisms is clearly described in the specification, e.g., at page 16, line 33- page 17, line 6 and in view of Figure 6. Hurtado does not require this TCH function or use of extension mechanisms because all of the playing functions and DRM functions of checking rights/decrypting content is all in the same player application and passed internally.

Third, with respect to the claimed User Interface Control Module element of the present invention, Claims 1, 6 and 10 are being amended to clarify that the user interface control module ensures that the user interaction with the player applications does not violate the usage rights. In the present invention, for example, this is accomplished by controlling or modifying the user interface of the player application, in a manner that is in accordance with the user's rights, such as described in the specification at page 19, lines 24, et seq. Particularly, this assurance is provided by controlling what is allowed or disallowed from the player application's user interface commands, e.g., hot keys, menu bar or tool bar options, pop-up menu options etc. For example, in the present invention, the user interface control module will disable buttons or menu choices (see specification at page 20, line 12 – page 25, line 10) to prevent access to functions that the user does not have rights for.

Respectfully, Hurtado does not teach this element. In support of the rejection, the Examiner claims Hurtado at col. 50, lines 66 - col. 51, line 4 teaches this element. However, the Examiner's reliance upon this passage is misplaced. The teaching in Hurtado cited by the Examiner is not relating to an interface control module for ensuring enforcement of user's rights, via the user interface, as implemented in the invention, but rather, teaches a manner in which a user may initiate a retransmission of purchased content, e.g., to address a possible scenario whereby a first transmission of purchased content is corrupted or not completely downloaded (See Hurtado at col. 51, lines 8-11). Respectfully, this is not suggestive of a user interface control module that ensures user interaction with the player applications does not violate the usage rights in accordance with the present invention as claimed in amended Claim 1, 6 and 10, for example, by disabling player application user interface buttons or menu choices.

Moreover, for clarification, Claims 1, 6 and 10 are being amended to set forth the feature that components of the verification system, trusted content handler, and user interface control module of the digital rights management system operate independently from the player application and reside locally in an end-user device having said player applications. That is, according to the invention, any end-user device having a player application, regardless of the player application version (e.g., even if upgraded to a newer version), may be provided with these DRM components of the invention as claimed without having the need to upgrade these DRM components; all that would be needed is the correct Trust Certificate to be generated for that correct player application version in order to validate the integrity thereof. Again, this is a feature of the invention clearly distinguished from the Hurtado system.

In sum, Hurtado does not have the off-line verification process and does not validate the integrity of the player application. Moreover, the TCH and user interface control

elements are local (downloaded to the end-user device) and operate independently of the player application. As such, Hurtado does not anticipate the present invention, and the Examiner is respectfully requested to withdraw the rejection of independent Claims 1, 6, and 10 and all claims directly or indirectly dependent thereon.

Moreover, with respect to the rejection of independent Claims 14, 18 and 20, as in the rejection of Claims 1, 6 and 10, the Examiner's reliance upon Hurtado is misplaced. These claims are directed to the details of the verification system and off-line process for validating a predefined property of the off-the-shelf player application, e.g., verifying a digest of the player application to ensure that it has not been modified. The Examiner, in the rejection of these claims, has cited Figure 1c) of Hurtado directed to the "Clearinghouse" element as teaching the issuance of a certificate generator. However, the certificate generated by the Hurtado system relates to the commerce or transaction integrity (e.g., verifying that the requesting end-user is a member of the "club" so that a sale or distribution of music to the end-user can take place), and not the integrity of the player application itself, i.e., that the player application exhibits a predefined property. Moreover, the code verifier element set forth in Claims 14, 18 and 20 relates to the player application program (i.e., "code" meaning a sequence of instructions) that is verified. Contrarily, the code referred to in Hurtado Figure 1d) is not a program code relating to the player application but is a code taken according to different context, e.g., a secret. For this reason, Hurtado can not be said to be anticipatory, and thus, the Examiner is respectfully requested to withdraw the rejection of independent Claims 14, 18 and 20 and all claims directly or indirectly dependent thereon.

In view of the foregoing remarks herein, it is respectfully submitted that this application is in condition for allowance. Accordingly, it is respectfully requested that this

application be allowed and a Notice of Allowance be issued. If the Examiner believes that a telephone conference with the Applicants' attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

Steven Fischman
Registration No. 34,594

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

SF:gc
Attachments: Annotated and Replacement Drawing Sheets